

# **EXHIBIT B**

**FOR OFFICIAL USE ONLY / LAW ENFORCEMENT SENSITIVE**

U.S. Department of Homeland Security

U.S. Citizenship and Immigration Services  
Office of the Director  
Washington, DC 20529



U.S. Citizenship  
and Immigration  
Services

## Memorandum

*Original Dated April 11, 2008*

TO: FIELD LEADERSHIP

FROM: Jonathan R. Scharfen, Deputy Director /S/

SUBJECT: Policy for Vetting and Adjudicating Cases with National Security Concerns

### I. Purpose

This memorandum outlines USCIS policy for identifying and processing cases with national security (NS) concerns,<sup>1</sup> and rescinds existing policy memoranda pertaining to reporting and resolving NS concerns. It also identifies Headquarters' Office of Fraud Detection and National Security (HQFDNS) as the point of contact for technical advice to assist the field<sup>2</sup> with vetting and adjudicating cases with NS concerns. This policy, known as the Controlled Application Review and Resolution Program (CARRP), establishes the following:

- The field is responsible for vetting and documenting Non-Known or Suspected Terrorist (Non-KST)<sup>3</sup> NS concerns, and adjudicating all NS-related applications and petitions.<sup>4</sup>

<sup>1</sup>A **NS concern** exists when an individual or organization has been determined to have an articulable link to prior, current, or planned involvement in, or association with, an activity, individual, or organization described in sections 212(a)(3)(A), (B), or (F), or 237(a)(4) (A) or (B) of the Immigration and Nationality Act (the Act). This determination requires that the case be handled in accordance with CARRP policy outlined in this memorandum.

<sup>2</sup> **Field** refers to Field Offices, Service Centers, the National Benefits Center, and equivalent offices within the Refugee, Asylum, and International Operations Directorate (RAIO).

<sup>3</sup> **Known or Suspected Terrorist (KST)** is a category of individuals who have been nominated and accepted for placement in the Terrorist Screening Database (TSDB), are on the Terrorist Watch List, and have a specially-coded lookout posted in TECS/IBIS, and/or the Consular Lookout Automated Support System (CLASS), as used by the Department of State. **Non-KST** is the category of remaining cases with NS concerns, regardless of source, including but not limited to: associates of KSTs, unindicted co-conspirators, terrorist organization members, persons involved with providing material support to terrorists or terrorist organizations, and agents of foreign governments. Individuals and organizations that fall into this category may also pose a serious threat to national security.

<sup>4</sup>This policy applies to all applications and petitions that convey immigrant or non-immigrant status. This policy does not apply to petitions that do not convey immigrant or non-immigrant status. See Operational Guidance for instructions.

**FOR OFFICIAL USE ONLY / LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy governing the use of FOUO information. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552). This document and the information contained herein are not to be distributed outside of DHS.

**Confidential - Subject to Protective Order** [www.uscis.gov](http://www.uscis.gov) **CAR000001**

**FOR OFFICIAL USE ONLY / LAW ENFORCEMENT SENSITIVE**Policy for Vetting and Adjudicating Cases with National Security Concerns  
Page 2

- The FDNS-Data System (FDNS-DS) is the primary system for recording vetting, deconfliction, and other resolution activities.<sup>5</sup>
- HQFDNS maintains responsibility for external vetting<sup>6</sup> of Known or Suspected Terrorist (KST) hits; and, upon request from the field, provides advice, technical assistance (including draft decisions), and operational support on KST and Non-KST cases with NS concerns.

II. Effective Date and Implementation

Operational Guidance implementing this policy will soon be issued by the Domestic Operations Directorate<sup>7</sup> (DomOps) and individual components of the Refugee, Asylum, and International Operations Directorate (RAIO). This policy will be effective upon issuance of each directorate's respective guidance.

III. Rescission of Prior Policy and Procedures

Upon issuance of the Operational Guidance, the following policy memoranda and procedures will be rescinded:

- *Processing of Applications for Ancillary Benefits Involving Aliens Who Pose National Security or Egregious Public Safety Concerns*, dated May 11, 2007;
- *Processing of Forms I-90 Filed by Aliens Who May Pose National Security or Egregious Public Safety Concerns*, dated May 11, 2007;
- *National Security Reporting Requirements*, dated February 16, 2007;
- *National Security Record Requirements*, dated May 9, 2006;
- *Permanent Resident Documentation for EOIR and I-90 Cases*, dated April 10, 2006;
- Appendix A of the Inter-Agency Border Inspection System (IBIS) [Standard Operating Procedure](#), dated March 1, 2006;

<sup>5</sup> If FDNS-DS is not currently available at any specific field office, officers must document CARRP procedures by another method as identified in Operational Guidance.

<sup>6</sup> **External Vetting** consists of inquiries to record owners in possession of NS information to identify: (a) facts or fact patterns necessary to determine the nature and relevance of the NS concern, including status and results of any ongoing investigation and the basis for closure of any previous investigation; and (b) information that may be relevant in determining eligibility, and when appropriate, removability. See section IV.C for further instruction.

<sup>7</sup> The **Domestic Operations Directorate** comprises Service Center Operations and Field Operations.

**FOR OFFICIAL USE ONLY / LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy governing the use of FOUO information. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552). This document and the information contained herein are not to be distributed outside of DHS.

**FOR OFFICIAL USE ONLY / LAW ENFORCEMENT SENSITIVE**Policy for Vetting and Adjudicating Cases with National Security Concerns  
Page 3

- *Revised Instructions for Processing Asylum Terrorist/Suspected Terrorist Cases*, dated January 26, 2005; and
- Section VIII of the Asylum Identity and Security Check Procedures Manual.

Officers should refer to relevant Operational Guidance<sup>8</sup> when adjudicating the following, *if found to involve NS or Egregious Public Safety*<sup>9</sup> concerns:

- Petitions that do *not* convey immigrant or non-immigrant status;
- Applications for employment authorization;
- Applications for travel authorization;
- Replacement Lawful Permanent Resident cards;
- *Santillan*<sup>10</sup> cases.

IV. Policy Guidance

This policy, in conjunction with Operational Guidance, provides direction to identify and process cases containing NS concerns in the most efficient manner. The process allows sufficient flexibility to manage the variety of cases encountered by USCIS.

Officers should note that at any stage of the adjudicative process described below, deconfliction may be necessary before taking action on a KST or Non-KST NS concern. Deconfliction is a term used to describe coordination between USCIS and another government agency owner of NS information (the record owner) to ensure that planned adjudicative activities (e.g., interview, request for evidence, site visit, decision to grant or deny a benefit, or timing of the decision) do not compromise or impede an ongoing investigation or other record owner interest.

A. Identifying National Security Concerns

As a result of the security checks<sup>11</sup> or at any stage during the adjudicative process, the

<sup>8</sup> Including [Policy Memorandum 110](#) (*Disposition of Cases Involving Removable Aliens*) issued July 11, 2006. That memorandum is not rescinded and does not apply to asylum applications.

<sup>9</sup> An **Egregious Public Safety (EPS)** case is defined in Policy Memorandum 110.

<sup>10</sup> *Santillan et al. v. Gonzales, et al.*, 388 F. Supp2d 1065 (N.D. Cal. 2005).

<sup>11</sup> **Security checks** may consist of the FBI Name Check, FBI Fingerprint Check, Treasury Enforcement Communications System/Inter-Agency Border Inspection System (TECS/IBIS), or United States Visitor and Immigrant Status Indicator Technology/Automated Biometrics Identification System (US VISIT-IDENT). Specific checks or combinations of checks are required for each application or petition type, pursuant to each component's procedures.

**FOR OFFICIAL USE ONLY / LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy governing the use of FOUO information. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552). This document and the information contained herein are not to be distributed outside of DHS.

**FOR OFFICIAL USE ONLY / LAW ENFORCEMENT SENSITIVE**Policy for Vetting and Adjudicating Cases with National Security Concerns  
Page 4

officer may identify one or more indicators<sup>12</sup> that may raise a NS concern. In such cases, the officer must first confirm whether the indicator(s) relates to the applicant, petitioner, beneficiary, or derivative (“the individual”).<sup>13</sup> When a Non-KST NS indicator has been identified, the officer must then analyze the indicator in conjunction with the facts of the case, considering the totality of the circumstances, and determine whether an articulable link exists between the individual and an activity, individual, or organization described in sections 212(a)(3)(A), (B), or (F), or 237(A) or (B) of the Act.

1. For Non-KST NS indicators, the officer should refer to the Operational Guidance for instruction on identifying those indicators that may raise a NS concern.
2. After confirming the existence of a KST NS concern via a TECS/IBIS check, the officer must contact the Terrorist Screening Center (TSC), as instructed in the content of the TECS/IBIS record, and must determine whether the KST NS concern relates to the individual. Officers are not authorized to request from the record owner any NS information related to a KST NS concern other than identification of the subject.

The officer must also consider and evaluate, in all cases, indicators related to family members or close associates of the individual to determine whether those indicators relate to the individual as well.

**B. Internal Vetting and Assessing Eligibility in Cases with National Security Concerns**

For both Non-KST and KST concerns, once the concern has been identified, the officer must conduct a thorough review of the record associated with the application or petition to determine if the individual is eligible for the benefit sought. The officer must also conduct internal vetting<sup>14</sup> to obtain any relevant information to support adjudication and, in some cases, to further examine the nature of the NS concern.<sup>15</sup>

For Non-KST NS concerns, the field is authorized to perform internal and external vetting. See step IV.C below for an explanation of external vetting.

For KST NS concerns, the field is only authorized to perform internal vetting. Record owners in possession of NS information are not to be contacted. HQFDNS has sole responsibility for external vetting of KST NS concerns.

<sup>12</sup> Guidelines for types of indicators that may be encountered during adjudication will be provided as an attachment to the Operational Guidance to assist officers in identifying NS concerns.

<sup>13</sup> For purposes of this memorandum, the term “individual” may include a petitioner.

<sup>14</sup> **Internal vetting** may consist of DHS, open source, or other systems checks; file review; interviews; and other research as specified in Operational Guidance.

<sup>15</sup> If an [exemption is granted under section 212\(d\)\(3\)\(B\)\(i\) of the Act](#) for a terrorist-related inadmissibility ground, and if no other NS concern is identified, no further vetting is necessary and the application may continue through the routine adjudication process.

**FOR OFFICIAL USE ONLY / LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy governing the use of FOUO information. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552). This document and the information contained herein are not to be distributed outside of DHS.

**FOR OFFICIAL USE ONLY / LAW ENFORCEMENT SENSITIVE**Policy for Vetting and Adjudicating Cases with National Security Concerns  
Page 5

The purpose of the eligibility assessment is to ensure that valuable time and resources are not unnecessarily expended externally vetting a case with a record owner when the individual is otherwise ineligible for the benefit sought. When this is the case, the application or petition may be denied on any legally sufficient grounds.<sup>16</sup>

When a NS concern exists, the NS information may be of a restricted or classified nature. These NS or law enforcement operations-based restrictions are often directly linked to protecting sensitive sources, methods, operations, or other elements critical to national security. Access to this information is therefore limited to those with a direct need to know and, when applicable, appropriate security clearance. As a policy matter, USCIS requires that a thorough eligibility assessment and completion of internal vetting precede any outreach for access to NS information.

C. External Vetting of National Security Concerns1. Non-KST NS Concerns

In a case with a Non-KST NS concern, the officer must initiate the external vetting process before the case may proceed to final adjudication if:

- the application or petition appears to be otherwise approvable, and internal vetting is complete;
- there is an identified record owner in possession of NS information; and
- the NS concern remains.

At this stage, the officer confirms with the record owner the earlier USCIS identification of the NS concern (*see* step IV.A above) and obtains additional information regarding the nature of the NS concern and its relevance to the individual. This is accomplished by obtaining from the record owner facts and fact patterns to be used in confirming whether an articulable link exists between the individual and an activity, individual, or organization described in sections 212(a)(3)(A), (B), or (F) or 237(A) or (B) of the Act.

Additionally, the officer seeks to obtain additional information that may be relevant in determining eligibility and, when appropriate, removability. This process requires close coordination with law enforcement agencies, the Intelligence Community,<sup>17</sup> or other record owners. If the external vetting process results in a finding that the NS concern no longer exists, and if the individual is otherwise eligible for the benefit sought, the application or petition is approvable.

<sup>16</sup> All references in this memorandum to “denying” a case also encompass the possibility of referring an asylum case to an Immigration Judge.

<sup>17</sup> Officers are not authorized to contact Intelligence Community members; such outreach is conducted by HQFDNS.

**FOR OFFICIAL USE ONLY / LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy governing the use of FOUO information. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552). This document and the information contained herein are not to be distributed outside of DHS.



**FOR OFFICIAL USE ONLY / LAW ENFORCEMENT SENSITIVE**Policy for Vetting and Adjudicating Cases with National Security Concerns  
Page 6

When USCIS obtains information from another government agency during the external vetting process, DHS policy guidance<sup>18</sup> requires that authorization from the record owner be obtained prior to any disclosure of the information. Therefore, in order to use the information during adjudication, prior written authorization must be obtained from the record owner. If the information indicates that the individual is ineligible for the benefit sought, and if permission from the record owner has been secured for the use of unclassified information,<sup>19</sup> the application or petition may be denied based on that unclassified information.

2. KST NS Concerns

For KST NS concerns, field officers are not authorized to conduct external vetting with record owners in possession of NS information. As stated above, only internal vetting of KST NS concerns is permitted at this stage. HQFDNS has sole responsibility for external vetting of KST NS concerns, which must be conducted in cases with a confirmed KST hit that have been determined to be otherwise approvable.

D. Adjudicating National Security Cases

Upon completion of required vetting, if the NS concern remains, the officer must evaluate the result of the vetting and determine any relevance to adjudication, obtain any additional relevant information (e.g., via a request for evidence, an interview, and/or an administrative site visit), and determine eligibility for the benefit sought. Adjudication of a case with a NS concern focuses on thoroughly identifying and documenting the facts behind an eligibility determination, and, when appropriate, removal, rescission, termination, or revocation under the Act.

If the individual is ineligible for the benefit sought, the application or petition may be denied.

If the vetting process results in a finding that the NS concern no longer exists, and if the individual is otherwise eligible for the benefit sought, the application or petition may be approved.

Non-KST NS Concerns

Officers are not authorized to approve applications with confirmed Non-KST NS concerns without supervisory approval and concurrence from a senior-level official (as

---

<sup>18</sup> See [DHS Management Directive 11042.1](#), *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*, dated 1-6-2005; and DHS Memorandum, *Department of Homeland Security Guidelines for the Use of Classified Information in Immigration Proceedings* (“[Ridge Memo](#)”), dated 10-4-2004.

<sup>19</sup> Requests for declassification of information and use of classified information during adjudication may only be made by HQFDNS. Officers should refer to Operational Guidance for further instruction.

**FOR OFFICIAL USE ONLY / LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy governing the use of FOUO information. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552). This document and the information contained herein are not to be distributed outside of DHS.

**FOR OFFICIAL USE ONLY / LAW ENFORCEMENT SENSITIVE**

Policy for Vetting and Adjudicating Cases with National Security Concerns  
Page 7

defined in Operational Guidance). That official also has discretion to request additional external vetting assistance from HQFDNS in accordance with Operational Guidance.

2. KST NS Concerns

Officers are not authorized to approve applications with confirmed KST NS concerns. If the senior-level official concurs, external vetting assistance must be requested from HQFDNS in accordance with Operational Guidance.

V. Conclusion

Officers should make every effort to complete NS cases within a reasonable amount of time, by taking into consideration the nature of the concern and the facts contained in each individual case. HQFDNS is available to provide technical expertise in answering questions that may arise in these cases. Any questions or issues that cannot be resolved in the field regarding identification, vetting, or adjudication of cases with NS concerns are to be promptly addressed through the established chain of command.

Distribution List:      Regional Directors  
                                District Directors  
                                Field Office Directors  
                                Service Center Directors  
                                Asylum Office Directors

**FOR OFFICIAL USE ONLY / LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy governing the use of FOUO information. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552). This document and the information contained herein are not to be distributed outside of DHS.

**Confidential - Subject to Protective Order** [www.uscis.gov](http://www.uscis.gov) **CAR000007**